ASSESSING RISK AND RESILIENCE FOR TRANSPORTATION INFRASTRUCTURE IN CANADA

William P. Anderson, Hanna Maoh and Charles Burke,
University of Windsor

Introduction

Goods producers in Canada rely on transportation networks to move raw materials and intermediate goods among production sites and finished goods to domestic and international markets. Firms in the retail, tourism and other service sectors also depend on transportation networks to assemble supplies and goods for sale and to bring customers to their facilities. Events that disable parts of the transportation network – ranging from weather emergencies to terrorist attacks – may therefore degrade economic productivity and in extreme cases may trigger economic crises. The ability of public and private providers of transportation infrastructure and services to mitigate and recover from such events is therefore an important determinant of aggregate economic performance.

This paper reviews analytical approaches for assessing the potential economic impacts of transportation infrastructure disruptions due to emergency events and provides some directions for methodological development. The next section reviews methods of risk assessment and discusses the concept of resilience. This is followed with a discussion of methods for measuring economic losses due to interruptions and for identifying the most critical links in an infrastructure system. The final section introduces a general framework for assessing resilience.

Risk Assessment and Resilience

The attacks of September 11, 2001 spurred development of assessment methodologies to help plan for emergency preparedness and to guide the distribution of public funds to the areas at greatest risk. This was especially true in the US, but similar initiatives have been undertaken in other countries, including Canada.[1] Methodologies that were already used for assessing the risk of natural events such as earthquakes and extreme weather were modified to include the terrorist threat. Basic risk assessment methodologies have been the subject of much criticism and major revisions over the past decade (Congressional Research Service, 2007.) Much of the confusion surrounding risk assessment arises from inconsistencies in the use of fundamental concepts, so a brief review is in order.

Risk may be simply defined as the expected value of the consequence C to society of some event with a probability p. If C and p are known, then risk may be calculated as $R=Cp$. If the consequence is measured in dollar terms and the probability is known, then the efficient level of public or private expenditure to prevent the event from occurring is any value less than or equal to R. (Naturally discounting would be employed if the probabilities and losses were defined over some time horizon.) In some analyses, a third variable, vulnerability(V), is added so that $R=CVp$. Here C represents consequences under normal circumstances and V is greater than or less than one depending upon the level of preparedness.

In practice, it is almost never that simple. Suppose the event in question is the explosion of a terrorist's bomb at a major port. The monetary consequences would include the cost of replacing the destroyed facilities as well as the system wide economic loss due to the disruption of the transportation services provided by that port. It is also likely that there would be loss of life due to the bombing as well as ecological damages as fuel and hazardous materials are released into the environment. While cost-benefit analysis typically translates such impacts into dollars, most public sector risk assessments avoid monetizing human lives and environmental impacts. Thus, C is a vector of impacts with different metrics. If V is included in the assessment, the problem becomes more complex, as a port may have

low vulnerability in terms of its physical design but the surrounding environment may be highly vulnerable.

Determining the value of *p* is even more problematic. For some types of emergency events, such as the occurrence of a hurricane, probabilities can be estimated based on past records. However, the probability must match not only the hurricane, but also the levels of *C*. So the "event" is not a hurricane, but rather a hurricane that results in consequence *C*. The consequences will depend not only on the severity of the storm but also on the point at which it makes landfall. This makes estimating *p* much more difficult. (If *V* is included it is even more difficult.)

Estimating probabilities for intentional events such as terrorist bombing involves even greater challenges, for two reasons. First, there is little history of such events in most places, so it is not possible to base probability on historical frequency. Second, intentional events are *adaptive threats* (Sheffi, 2005; Cox, Prager and Rose, 2011). The fact that an attack has occurred on a particular type of facility in the past does not necessarily mean that an attack on the same type of facility is likely in the future. The perpetrator will anticipate that authorities will increase their protection of the class of facility that have already been attacked, and therefore choose a different class of facility where the perceive probability of attack is lower. Furthermore, he will also target those places with the highest values of *C* and *V*. For this reason terrorist attacks fit Taleb's (2010) definition of a *Black Swan*: a low probability event that has major consequences and which is virtually unpredictable.

Given these complexities, most risk assessments do not attempt to produce a cardinal measure of risk. Instead, the risk of any event is defined as depending on a number of characteristics of the event that are closely related to *p*, *C* or *V*. Event scenarios are rated on these characteristics and some sort of weighting or similar methodology is applied to produce a single value that serves as an ordinal measure of risk. In this way, risk can be compared across event types, regions, and infrastructure elements in order to identify the threats that present the highest risk. This process, for all its shortcomings, at least

compels decision makers to compare possible threats on a set of objective criteria and define a subset of threats on which resources should be concentrated. (See FEMA 2005 for a detailed description of risk assessment process.)

Once the events that pose the highest risk are identified, a number of policies may be enacted to reduce their risk levels. This may include actions to reduce either p or C. (In principle, most of the second category actually address vulnerability, but to keep things simple we assume that C is a function of vulnerability, so reducing V reduces C.) Reducing the probability of occurrence is not possible in some cases, specifically natural disasters such as earthquakes or hurricanes. However, a variety of policies can be used to reduce the probability of terrorist and other intentional events, including intelligence and law enforcement activities and the erection of physical barriers intended to thwart such events before they occur.

Strategies for reducing consequences can be organized under three categories:

1. *Hardening*: making physical assets more damage resistant.
2. *Response*: improving the ability of first responders to limit damage immediately following the event.
3. *Resilience:* improving the ability of infrastructure and other affected systems to "bounce back".

Hardening includes measures such as building codes to fortify construction in earthquake zones, seawall construction in areas vulnerable to storm surges and any protective elements that can limit damage around likely terrorist targets. Hardening can also include "soft" measures, such as excluding construction from flood zones. Response refers to the capability of police, fire, emergency medical and other first responders to save lives and property in the first hours and days after the event. Hardening and response combine to produce robustness, the ability to withstand shocks with limited damage.

Resilience is a term that has gained currency in recent years. But a review of the literature shows that it is used in a variety of different

ways. A recent joint declaration of the President Obama and Prime Minister Harper uses it in a very broad way: "We intend to strengthen our resilience – our ability to mitigate, respond to, and recover from disruptions."[ii] This would include both hardening and response. By contrast, Cox, Fynnwin and Rose (2011) insist that resilience applies only to measures that are implemented after an event. Thus, it applies only to the "recover from" in the joint declaration. Others define resilience as the ability to absorb shocks from extreme events (McDaniels *et al*, 2008) or the ability of a system to maintain function while shocked (Rose, 2007).

The basic idea that underlies most definitions of resilience is as follows. An extreme event such as a hurricane or a terrorist bomb will inflict damage on a system. The extent of the damage will depend upon the severity of the event and the effectiveness of hardening and response. Resilience refers to two things: 1) how well the system can function for a given level of damage and 2) how quickly it can be restored to its pre-event state. Consider the case of a highway system in which a large capacity bridge has been destroyed as the result of a natural disaster or intentional attack. The resilience of that system will be expressed in terms of 1) its ability to accommodate car and truck traffic while the bridge is out of services, and 2) the speed at which the infrastructure owner (public or private) can replace the bridge or provide other infrastructure that provides a comparable capacity.

What factors give rise to resilience? Sheffi (2005), while referring to resilience in firms, argues that resilience is produced either via *redundancy* or *flexibility* (or a combination of the two.) For a firm, redundancy includes things like excess inventory and spare production capacity. Flexibility includes the ability to find alternatives to disrupted suppliers and markets, to re-task existing assets and to adjust product lines. Since redundancy is inefficient under normal circumstances, resilience via flexibility is the preferred strategy.

Applying these concepts to a highway system, redundancy may refer to the ability to move between origins and destinations via a large

number of routes. Specifically, a high level of redundancy is associated with the absence of critical links such as bottlenecks that can greatly reduce the quality of transportation service if disabled. Studies have shown that the negative impact of highway infrastructure failures due to earthquakes can be significantly offset by a high degree of redundancy (Gordon, Richardson and Davis, 1988.) Other things being equal, redundant networks are resilient networks. Furthermore, in the case of transportation networks, redundancy is not necessarily a dead loss during normal times because it may reduce circuity[iii] and congestion.

It may seem that there is little scope for resilience via flexibility in a highway network. A few adjustments are possible, such as re-tasking HOV lanes as freight lanes, but for the most part assets are set in the ground and not very flexible. But the picture changes if you think of the highway system as comprising not only the infrastructure network and its provider, but also vehicles and the households, shippers and carriers who operate them. Shippers and carriers can make decisions to work around disabled highway elements by sourcing from different places, shifting some shipments to rail or reassigning their internal assets to use inputs they can get and to serve markets they can reach. The key is for the infrastructure provider to make sure carriers and shippers have detailed and current information on closures, detours, traffic conditions, etc. For this reason, a recent Freight Resilience Plan for the State of Washington emphasised the provision of timely information on system conditions to users as one of the most effective ways for the Department of Transportation to achieve resilience (Ta, Goodchild and Ivanov, 2010; MIT, 2009).

Assessing Economic Loss

Economic loss due to infrastructure disruption is one of the most important, although certainly not the only, component of the consequences measured in a risk assessment. Looking at the components of economic loss provides a useful illustration of the importance of resilience.

When an element of a transportation infrastructure network such as a bridge, roadway, track or tunnel, is damaged or destroyed and its services is interrupted, the system-wide economic losses fall into two categories. The first category, which we call *direct loss*, is associated with the cost of emergency response and damage to the facility and is generally borne by public safety agencies and the firm or agency that owns and operates infrastructure. The *indirect loss* is associated with the loss of the services of the facility and can be quite broadly spread throughout the economy.

As an example, suppose a bridge is damaged by an earthquake and has to be closed for an extended period while repairs are done. The direct loss includes the cost of response, which falls on first responder agencies, and the cost of implementing the repairs, which would fall on the provincial ministry, the municipality, a bridge authority or a private firm, depending upon who owns the bridge. We might also include the cost of any vehicles and their cargos lost because they were on the bridge at the time of the earthquake. (Naturally, any loss of life would be the most significant consequence, but we are treating that as separable from economic loss.) The most important policy response for reducing direct loss would be hardening, which in this case would mean either building or retrofitting the bridge to make it more resistant to earthquakes.

The indirect loss is borne by all regular users of the bridge who will now have to make alternative arrangements for the lost service. This includes both the drivers of cars who use the bridge to reach jobs, school, shopping, recreation, etc. and the operators of trucks who use the bridge to move goods from producers to purchasers. In reality the magnitude of the indirect loss will depend on a variety of factors related to the nature of the local economy and the ability of households to substitute among sources of purchases, economic activities and destinations. (The highly developed US HAZUS Model treats these substitutions explicitly in estimating economic loss associated with earthquakes and other disasters.[iv]) But for the sake of argument, assume that we can capture all indirect loss in terms of the cost of traffic delay. The magnitude of the indirect loss will depend on the following factors:

1. The redundancy of the transport network
2. The excess capacity in the network
3. The length of time over which the bridge is closed.
4. The value of time

Clearly factors 1 through 3 are indicators of the resilience of the highway network of which the bridge is a part.

We can illustrate with a simple numerical example. Suppose the bridge in question is a steel beam construction 100m long and 15m wide. According to the British Columbia Ministry of Transportation and Infrastructure (2010), the replacement cost for such a bridge is about $9,000,000. To this we add one million to cover response cost, so the total direct cost is $10,000,000. Assume that the highway segment on which the bridge is located has an annual average daily traffic (AADT) of 15,000. We estimate total delay per day by multiplying AADT by the average delay. We then estimate indirect cost per day by multiplying the total delay times the value of time.

Assume the value of time is $15/hr for cars and $70/hr for trucks.[v] The Canadian average ratio of one truck per 27 cars yields a weighted average of just over $17 per hour. The average delay will depend principally on redundancy. If the bridge in question is a major bottleneck with no nearby alternative, the delay will be high because the cars and trucks will have to travel a long distance to find an alternative bridge. Even if there is a nearby bridge, the detour routes leading to that bridge and the bridge itself may not have sufficient capacity to carry the additional traffic without significant congestion, which will further increase delay time. Thus, effective redundancy depends not only on the structure of the network but also on the capacity of its links. For the sake of our example, we define a high redundancy scenario as 15 minutes delay per vehicle and a low redundancy scenario as 45 minutes delay.

The total indirect loss also depends on the time it takes to replace the bridge. For our example we use two scenarios: a very optimistic value of 90 days and a more realistic estimate of 180 days. In fact, this time

could be much longer. The results of calculations for the hypothetical example are shown in Table 1.

Table 1: Economic Loss for Hypothetical Example

Redundancy	Recovery Time	Direct Loss ($000)	Indirect Loss ($000)	Total ($000)
High	90 days	10,000	5,749	15,749
Low	90 days	10,000	17,247	27,247
High	180 days	10,000	11,499	21,499
Low	180 days	10,000	34,495	44,495

This rather crude example is subject to a variety of criticisms, but it is only intended to illustrate a couple of important points. The first is that under all but the most optimistic assumptions about redundancy and recovery time, indirect loss is equal to or greater than direct loss. This means that any risk assessment that does not take full account of indirect loss is probably missing most of the economic consequences. The second is that the indirect loss – and therefore the total economic loss—is highly sensitive to redundancy and recovery time, both of which are factors that come under the heading of resilience.

This is consistent with the general observation in a recent MIT (2009) study for the State of Washington, that the economic impacts of poor recovery can be much larger than the initial impact of natural disaster or terrorist attack. The study goes on to note that US states have devoted far more resources to planning for initial response than to planning for recovery. The situation in Canada is probably similar.

Identifying Critical Elements

In light of the important role of resilience in assessing vulnerability of a transportation system to disruptions due to extreme events, it is import to be able to assess the level of redundancy in a road network or other transportation network. In a crude sense it is possible to assess redundancy by a single measure that applies to an entire network. Consider a network with n nodes (which may be defined as points of origin and destination) and l links (road segments between nodes). A minimum number of links $l=n-1$ is necessary to achieve full connectivity. If $l>n-1$ there is some redundancy in the sense that

pairs of nodes can be connected by more than one sequence of links. Thus the ratio *l/n* is a crude measure of redundancy. This is not a very useful metric, however, because even networks with high ratios can have individual links for which there is little or no redundancy. Such links are commonly called bottlenecks.

Scott *et al* introduced a metric called the Network Robustness Index (NRI) that is applied to specific links to indicate their criticality to a network. Assume that each link *a* on a network has a performance function $t_a(x_a)$ relating link travel time *t* to link flow *x*. A user equilibrium model can be used to assign flows to all links based on a matrix of origin-destination flows. A global measure of network performance can then be calculated as

$$c = \sum_a t_a x_a$$

Calculation of the NRI starts by removing a specific link *a*, repeating the user equilibrium assignment and defining a new performance measure

$$c_a = \sum_a t_a x_a \delta_a$$

where δ_a is set to zero for the link that was removed and 1 for all other links. The NRI is then defined as

$$q_a = c_a - c.$$

In words, the NRI is the extra travel time that is imposed on the network because of the removal of a particular link. This is a very valuable measure because it can be used to identify the most critical links in the network, which may therefore be the best candidates for hardening. (As Scott *et al* points out, this method gives substantially different results than the traditional approach as defining the link with the highest ratio of flow to capacity as the most critical link.)

It also tells us something about redundancy because a high NRI means that there is little redundant capacity for the link in question. It does not, however, tell us what links in the network serve the important purpose of providing redundancy. For example, a road segment may rank low in terms of both the NRI and the ratio of flow to capacity, but may still contribute valuable redundancy.

With this in mind, a useful complement to the NRI would be a redundancy value (RV) metric. For a particular link *b* define

$$c_{ab} = t_a x_a \delta_a \delta_b$$

This is the performance of the road network with both links *a* and *b* removed. The redundancy support that link *b* provides to link *a* is measured as

$$r_{ab} = c_{ab} - c_a \, .$$

The redundancy value of link *b* to the entire network is then defined as

$$r_b = \sum_a r_{ab} \, .$$

While the value r_b has no intuitive meaning, it can be used to rank road segments in terms of the redundancy they contribute to the network. It can also be used to assess any proposed new links in terms of their contribution to redundancy.

A Framework for Assessing Resilience

The full specification of a quantitative model capable of assessing risk and resilience in a broad transportation system, such as a provincial highway network, is beyond the scope of this paper. Based on the foregoing discussion, however, we can identify some basic requirements for such a model and sketch out a framework for its development.

The basic model requirements include the following:

1. *The model must be able to generate a large number of network disruption scenarios.* Since all extreme events are hard to predict, and terrorist events are almost impossible to predict, the best strategy is to generation numerous scenarios, each of which involves the lost of one or more network links. This involves running the model hundreds or even thousands of times, with the goal of assessing system performance under the broadest possible range of scenarios and identifying areas of significant (and perhaps unforeseen) vulnerability.
2. *The network and its users should be modelled as an integrated system.* Resilience arises from redundancy, which is principally built into the infrastructure systems, and flexibility, which is principally accomplished through decisions and substitutions made by its users. In particular, a model in which freight users' decisions are exogenous cannot capture resilience. This implies that the model must incorporate elements of supply chain management that are absent from most transportation planning models.
3. *The model must be dynamic.* Defining the state of the system pre-event, post-event and post-recovery is not sufficient. It must be possible to estimate recovery trajectories. For example, a system may take a year to recover 100% of its function after a disaster, but it is more resilient if it recovers 80% after the two months than if it recovers 50%.

A general model framework is shown in Figure 1. It includes a module for generating a large number of emergency scenarios based on information about vulnerabilities but with a random component. Each scenario is defined in terms of the loss of network elements. The transportation system module includes a network algorithm to determine the effect of the lost elements in terms of reassignment of traffic and congestions and to identify those parts of the network that lose services. Information on changes in network performance is exchanges with an economic module that estimates both the immediate economic impacts of the degradation of transportation

system performance and adjustments that users make as they are faced with more limited transportation options. The latter are passed back to the transportation system module to see how those adjustments affect system performance.

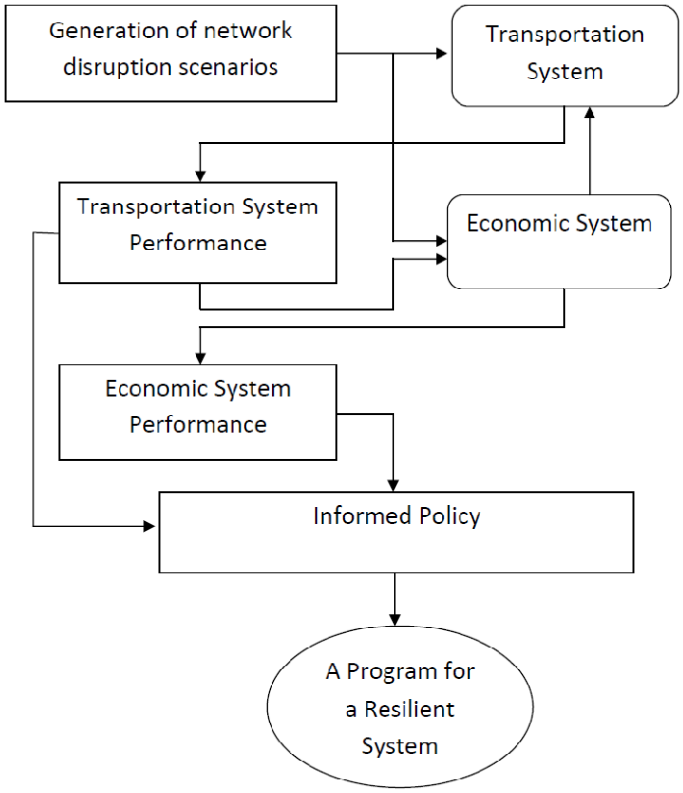

Figure 1: Model Framework for Assessing Risk and Resilience

The dynamics of the model are driven by two processes. The first is the process of adjustment by system users. For example, some production units may be shut down immediately following an event

because of lost access to inputs, but may come back into service as alternative input sources or transport modes are found. The second is through the restoration of lost links by the system infrastructure provider. This means that the model must be capable of estimating restoration times for various categories of infrastructure.

Naturally, the goal of such a modelling system is to inform policy. Decision makers will be provided with estimates of transportation system performance and the performance of the overall economy under a broad range of scenarios. Policy steps such as hardening vulnerable infrastructure elements, adding redundant links or expanding links that provide redundancy, designating freight-only lanes in emergency situations and even non-transportation policies such as favourable tax treatment for emergency inventories can be represented in the model and all scenarios re-run in order to judge their effectiveness in reducing risk and increasing resilience.

References

Cox, Andrew, Fynnwin Prager and Adam Rose (2011) Transportation security and the role of resilience: a foundation for operational metrics, *Transport Policy*, 18:307-317.

Federal Emergency Management Agency (2005) *Risk Assessment: A How-to Guide to Mitigate Potential Terrorist Attacks Against Buildings*, Washington: US Department of Homeland Security. (FEMA 452).

Government of Canada (2009) *National Strategy for Critical Infrastructure*, Ottawa: Her Majesty the Queen in Right of Canada. (Cat. No. PS4-65/2009E-PDF).

McDaniels, Timothy, Stephanie Chang, Darren Cole, Joseph Mikawoz and Holly Longstaff (2008) Fostering resilience to extreme events within infrastructure systems: Characterizing decisions contexts for mitigation and adaptation, *Global Environmental Change, 18:310-318.*

MIT Center for Transportation and Logistics (2009) *Development of a Statewide Freight System Resilience Plan: Final Report*, Cambridge, MA: Massachusetts Institute of Technology.

Rose, Adam (2007) Economic resilience to natural and man-made disasters: Multidisciplinary origins and contextual dimensions, *Environmental Hazards*, 7:383-398.

Scott, Darren, David C. Novak, Lisa Aultman-Hall, and Feng Guo (2006) Network robustness index: A new method for identifying critical links and evaluating the performance of transportation networks, *Journal of Transport Geography*, 14:215-227.

Sheffi, Yosi (2005) *The Resilient Enterprise*, Cambridge, MA: The MIT Press.

Ta, Chilan, Anne V. Goodchild and Barbara Ivanov (2010) Building resilience into freight transportation systems, *Transportation Research Record*, 2168:129-135.

Taleb, Nassim Nicolas (2010) *The Black Swan: The Impact of the Highly Improbable* (second edition), New York: Random House.

---

[i] For example, Canada's strategy for critical infrastructure calls for risk assessments. (Government of Canada, 2009).

[ii] "Beyond the Border: a shared vision for perimeter security and economic competitiveness." Available at http://www.pm.gc.ca/eng/media.asp?id=3938

[iii] "Circuity" refers to the average ratio of the network distance to the straight line distance between points.

[iv] HAZUS documentation may be found at http://www.fema.gov/plan/prevent/hazus/

[v] This is roughly consistent with values used in the recent report from the Chicago Metropolitan Planning Council, "Moving at the Speed of Congestion: the true costs of traffic in the Chicago Metropolitan Area" available at http://www.metroplanning.org/multimedia/publication/272